United Nations E/CN.15/2014/7

Economic and Social Council

Distr.: General
5 March 2014

Original: English

Commission on Crime Prevention and Criminal Justice
Twenty-third session
Vienna, 12-16 May 2014
Item 7 of the provisional agenda*
World crime trends and emerging issues and responses in the field of crime prevention and criminal justice

Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children

Report of the Secretary-General

Summary

The present report was prepared pursuant to Economic and Social Council resolution 2011/33 on prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. In that resolution, the Economic and Social Council requested the United Nations Office on Drugs and Crime to carry out a study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children. This report includes a summary of the main findings of the study and an assessment of the needs of States for training in the investigation of offences against children committed by using new information and communication technologies, as also requested in resolution 2011/33.

* E/CN.15/2014/1.

V.14-01456 (E) 210314 240314

Please recycle

I. Introduction

1. The present report is submitted to the Commission on Crime Prevention and Criminal Justice at its twenty-third session, pursuant to Economic and Social Council resolution 2011/33 on prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. In that resolution, the Economic and Social Council requested the United Nations Office on Drugs and Crime (UNODC) to carry out a study facilitating the identification, description and evaluation of the effects of new information and communication technologies on the abuse and exploitation of children.

2. In that resolution, the Council also requested UNODC to design and carry out an assessment of the needs of States for training in the investigation of offences against children committed by using new information and communication technologies and, on the basis of the results of that survey, to design a training and technical assistance programme to assist Member States in combating such offences more effectively, subject to the availability of resources and not duplicating the efforts of the International Criminal Police Organization (INTERPOL).

3. This report includes a summary of the main findings of the study and the assessment of the needs of Member States for technical assistance, in particular, training of law enforcement personnel in the investigation of offences against children committed using new information and communication technologies.[1] As requested by the Economic and Social Council in its resolution 2011/33, the study and the assessment of needs take into account relevant data collected by the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, as well as relevant studies carried out by regional organizations and other organizations within the United Nations system, such as the United Nations Children's Fund, the International Telecommunication Union and the Office of the United Nations High Commissioner for Human Rights. In addition, the preparation of the study and needs assessment were facilitated by an informal expert group meeting held in September 2013. The informal expert group meeting brought together international experts from the fields of law enforcement, research, industry and civil society.

II. Study to facilitate the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children

A. Background

4. Several factors have given rise to increasing concern over the effects of new information and communication technologies on the abuse and exploitation of children. In recent decades, innovation in those technologies has transformed societies worldwide. By the end of 2012, more than one third of the world's

[1] The full study is contained in E/CN.15/2014/CRP.1. Information on the training and technical assistance programme is made available in E/CN.15/2014/CRP.2.

population, more than two billion people, had access to the Internet.[2] Other innovations include dramatically increased levels of access to computers, faster transmission speeds and the mobilization of devices. Children adopt these technologies at an earlier age than in the past, and at a certain point, going online has become thoroughly embedded in children's lives.[3] Eighty per cent of children in the European Union between the ages of 5 and 14 years use mobile telephones.[4]

5. While use of information and communication technologies is widespread among children, they often lack knowledge of the appropriate protective measures relating to the sharing of information, photos and videos. In addition, children who are accustomed to a culture that thoroughly integrates information technology may not draw a distinction between online and offline "friends". At the same time, information and communication technologies are increasingly used for the commission of crime. Organized criminals are highly innovative and have quickly adopted new technologies and modalities for crime, including in areas such as online extortion and the use of technology for the recruitment of victims for trafficking in persons, or sexual exploitation. In the future hyperconnected society, many crimes will most likely contain at least one digital component, placing children at significant potential risk.

6. Technology, and our relationship to it, is constantly evolving. In its resolution 2011/33, the Economic and Social Council specifically expressed concern that increasingly rapid technological advances have created new possibilities for the criminal misuse of new information and communication technologies. At the same time, it is important to note that, in the midst of technological transformation, not all forms of abuse and exploitation facilitated by those technologies are necessarily different from previous forms of abuse and exploitation. While some genuinely new forms may arise, many forms of child abuse and exploitation involve the same dynamics, issues and concerns whether they are initiated online or through offline channels. The present report concludes that the keys to fighting technology-facilitated abuse and exploitation are awareness-raising, proactive investigation and training of practitioners on gathering, preserving and presenting electronic evidence.

B. Identifying and describing the problem

7. Owing to the comparatively recent emergence of forms of cybercrime and, specifically, child abuse and exploitation facilitated by information and communication technologies, internationally agreed definitions of these phenomena are still evolving. Terminology used in this report seeks to provide an effective description of conduct and acts without aiming to provide final or definitive definitions.

---

[2] International Telecommunication Union, *World Telecommunication/ICT Indicators database*, 17th ed. (Geneva, 2013). Available from www.itu.int.

[3] Child Exploitation and Online Protection Centre, "Threat assessment of child exploitation and sexual exploitation and abuse" (London, 2013), para. 14.

[4] International Telecommunication Union, *Use of Information and Communication Technology by the World's Children and Youth* (Geneva, 2008).

8. The forms of abuse and exploitation of children that have been most affected by technological innovation include various forms of conduct involving child sexual abuse material; commercial sexual exploitation of children; cyberenticement; an array of problematic online conduct that includes cyberharassment, cyberstalking, and cyberbullying; and the use of information and communication technologies to expose children to harmful content.

9. Many scholars and practitioners advocate using the term "child sexual abuse material" as opposed to "child pornography", asserting that it promotes a better understanding of the nature of the crime and affords more respect to victims. Such advocates hold that depictions of children engaged in sexual activities are always abusive or exploitative. At its core, child sexual abuse material consists of a recording, usually in the form of a visual image or video, that depicts a child engaged in explicit sexual activity. Several international instruments deal with child sexual abuse material, which can be defined as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."[5] Child sexual abuse material takes many different forms, including photographs, negatives, slides, magazines, books, drawings, movies, videotapes and computer disks or files.

10. In the realm of commercial sexual exploitation of children, two kinds of offences have been particularly affected by the increased use of information and communication technologies: trafficking in children for the purposes of sexual exploitation and the abuse and exploitation of children in the travel and tourism industries. Trafficking in persons is defined in the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, as the recruitment or other enumerated act, by means of the threat or use of force or other enumerated means, for the purpose of exploitation (art. 3). It is important to note that the "means" element of the crime is considered irrelevant in the case of a child victim. In other words, a child, and even the child's parents, can never consent to the child being trafficked or exploited because of the special legal status afforded to children.

11. Child abuse and exploitation in the travel and tourism industries involves the commercial sexual exploitation of children by men or women who travel from one place to another, domestically or internationally, and engage in sexual acts with a child, defined as anyone under the age of 18 years. Child sex tourists may be preferential abusers, who deliberately seek out children for sex, or may be situational abusers, who take advantage of an opportunity or a feeling of anonymity afforded by travelling.

12. The terms "cyberenticement", "solicitation" and "online grooming" are often used together or interchangeably to refer to conduct by adults, through or with the use of information and communication technologies, for the purpose of sexually abusing or exploiting a child. Each of those terms, however, has a distinct denotation. "Cyberenticement" refers to the persuading, soliciting, coaxing, enticing, or luring by words, actions or through communication on the Internet or

[5] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (United Nations, *Treaty Series*, vol. 2171, No. 27531), art. 2 (c).

any electronic communication, of a minor for the purpose of engaging in sexual conduct. "Solicitation of children for sexual purposes" refers to an intentional proposal, through information and communication technologies, by an adult, to meet a child who has not reached the age of majority set in domestic law, for the purpose of committing sexual abuse or producing child pornography where this proposal has been followed by material acts leading to such a meeting. "Grooming" refers to a series of acts that facilitate cyberenticement such as actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to overcome the child's resistance in preparation for sexual activity with the child.

13. Information and communication technologies also facilitate an array of problematic conduct that is sometimes but not always criminalized. The lines between these forms of conduct can be difficult to delineate. "Cyberharassment" commonly refers to the intimidation, repeated or otherwise, of one individual by another person or a group, perpetrated using electronic means. Cyberstalking is characterized by the repetitive nature of the conduct and is often understood as a course of action that involves more than one incident, perpetrated using electronic means that causes distress, fear or alarm. Like its offline predecessor, cyberstalking includes activities related to locating, surveying and, often, harassing or manipulating a victim or victims.

14. Much like cyberharassment and cyberstalking, cyberbullying encompasses the use of information and communication technologies to harm a victim or victims in deliberate, repeated and hostile ways. This can include the use of the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person. Some approaches to characterizing the phenomenon refer to the age of the victim and perpetrator, such as when a child, pre-teenager or teenager is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, pre-teenager or teenager using the Internet, interactive and digital technologies or mobile phones.

15. "Harmful online content" is a very broad category that includes any online material that has the ability to negatively influence children. Examples include online pornography and especially child sexual abuse material, violent video games and websites that espouse racial or ethnic hatred and commercial sites that seek to swindle youth or steal their identities. Children may be exposed to harmful content as the result of deliberate searches or inadvertent contact resulting from search queries, pop-up advertisements or e-mails received from spam operators. Some websites and games use age restrictions and checks to ensure that children are not exposed to harmful content. However, often there are few real barriers to prevent children from accessing the content at a younger age.

C. Evaluating the problem

16. In evaluating the effects of new information and communication technologies on the abuse and exploitation of children, a continuum of effects emerges. Some conduct facilitated by those technologies shares many features and similarities with forms of abuse and exploitation already known and can be countered in familiar ways. In some instances, the effect of technology on an existing form of abuse and

exploitation is so transformational that it must be prevented and countered in new ways. In a few cases, the use of new information and communication technologies has given rise to completely new forms of child abuse and exploitation. The use of information and communication technologies in the commission of offences can increase the levels of harm to victims, in particular by facilitating the layering and intertwining of offences so that multiple forms of abuse and exploitation facilitated by those technologies can take place simultaneously or be committed against the same victim over time.

1. Enhanced access to victims and abuse material

17. Perpetrators use information and communication technologies to gain access to children more easily and in greater numbers than they could if acting in person, through the use of online forums, e-mail, social networks and other Internet-based communications. Technology has also made new populations of children accessible to offenders, as mobile telephone use has grown, especially in developing countries. In particular, such platforms allow perpetrators to interact with many potential victims simultaneously. Some offenders have up to 200 children whom they are at various stages of grooming at one time. With such a large pool of potential victims, predators can bear the risk of testing the waters with their targets by initiating sexual conversations. They then focus on those that respond favourably or at least remain engaged, enabling predators to allocate their time to building "relationships" with higher probability targets. In doing so, offenders rely on the absence of interpersonal cues in the online environment, which has the effect of undermining the ability of children to protect themselves.

18. Information and communication technologies also enable perpetrators to have increased access to information about victims or potential victims. Social networking sites contain tremendous quantities of personal and biographical information. The technology used in such sites and mobile applications can also integrate a great deal of additional information such as the location where pictures were taken. Added to the inherent risk of such information-sharing is the fact that children act on a false sense of privacy and safety in sharing pictures and data about themselves. Even those who attempt to protect their privacy and security struggle to keep abreast of the frequently changing privacy policies of social media sites. New features such as geo-tagging of images and "checking-in" to places via mobile device further increase offenders' physical access to children. Services and applications that merge technological functionality make the task of gathering information even easier. For example, the social media tool "Cree.py" culls information associated with a single e-mail address from photo-sharing, social media and other sites to create a dossier of information that can include a child's whereabouts. In addition, while most sites and applications take steps to ensure cybersecurity, personal information remains vulnerable to compromise through hacking and illegal access.

19. Offenders use information and communication technologies to break down both physical and psychological barriers to abusing or exploiting children. Many social networking sites effectively enable users to conceal their real identity. Predators may adopt false identities to lure child victims into an online relationship. Once children feel emotionally attached, offenders can more easily reveal their true identities and still maintain the loyalty of their victims. Some predators also make

use of pornography or child sexual abuse material to remove psychological barriers and convince their targets that child abuse is normal. Offenders may try, for example, to use child sexual abuse material in an attempt to sexualize, celebrate or legitimize acts such as rape, battery, sexual harassment, prostitution or child sexual abuse.

20. With respect to victims of trafficking, pimps, madams and escort agencies recruit new victims through their own websites, as well as using social media technology to advertise their services widely. Travelling sex abusers use chat rooms, message boards, peer-to-peer file-sharing servers, news groups and specialized websites to obtain information on potential destinations and victims, share stories, trade child sexual abuse material and plan travel.

21. As a fast, free and difficult-to-trace means of obtaining and sending content, information and communication technologies provide increased opportunities for offenders to send harmful content to children. A particular source of unwanted harmful content involves peer-to-peer files. Offenders mislabel files to trick children into opening them. Files containing violent child sexual abuse material may be given the name, for example, of video clips from popular movies aimed at young people. As a result, children may unwittingly download and view them.

2. Increased profits for criminal enterprises

22. Advances in information and communication technologies have increased profits for criminal enterprises that abuse and exploit children. In the past, producers of child sexual abuse material had to use expensive film and copying equipment and then ship physical copies on videotape or CD-ROM. Moreover, to solicit customers, producers needed to invest in print advertisements. Owing to the public nature of such advertisements, offenders used cryptic language and terms so as not to alert law enforcement authorities. That often had the effect of restricting the distribution of such material and the resultant profit.

23. In the current environment, information and communication technologies reduce the cost and effort of all aspects of criminal entrepreneurship. Digital equipment creates a cheap and easily accessible means of producing and widely distributing child sexual abuse material. Commercial spam operations reduce the challenge and cost of e-mail distribution, such that the scale of illicit operations can quickly be expanded. Once linked with customers, offenders can continuously advertise additional illicit materials in open and explicit language. Perpetrators can also keep in touch with customers freely, enabling them to offer new material over time, thus generating more revenue.

24. Perpetrators no longer need to find HTML programmers to create websites, as they did just a decade ago. Rather, they can now employ one of many "drop-and-drag" platforms to build feature-rich sites. Step-by-step guides, which can be found with a simple web search, detail the set-up and maintenance of a hidden, anonymous website on the Tor network or the "dark web". With even less effort and expense and some basic precautions, offenders can make use of photo-sharing, banner advertising and social networking applications to host graphic content.

25. The cost-saving benefits derived from information and communication technologies also facilitate commercial sex trafficking enterprises, including those

involving children. Mobile telephone technology connects offenders, victims and consumers, thereby reducing the need for offenders to be physically present at transactions. Offenders are able to recruit, advertise, organize and communicate primarily, or even exclusively, via mobile phone, effectively streamlining their activities and expanding their criminal networks. At the same time, operators of illicit businesses are frequently able to charge travelling offenders more money for the service of facilitating encounters at almost any time and on short notice.

3. Reduced risk of detection

26. The use of information and communication technologies in the abuse and exploitation of children has also, in some ways, reduced the risk of detection. The use of mobile phones, e-mail and messaging applications enables offenders to hide their identities and conceal their offences. Offenders can purchase disposable phones or pay-as-you-go SIM cards in cash transactions, which do not require any form of registration. E-mail accounts may be registered using false identities and multiple proxies and be made from public wireless hotspots, making it extremely challenging to link an account registration with a particular individual. Many Internet cafes offer a substantial degree of anonymity because they do not require identification to log in to computers, do not use monitoring systems of any kind and do not have enforced codes of conduct.

27. Further, with the rise of mobile "smart" phones, offenders can commit offences in a greater range of locations than would be possible with a full-size computer or even a laptop. Offenders may both record and distribute child sexual abuse material, for example, solely from their mobile telephone. Cyberstalkers can also harass their victims with less effort and lower risk by exploiting information and communication technologies. In the past, stalkers might attract attention when using public telephones to make harassing phone calls. However, with new technology, cyberstalkers can operate from almost anywhere. Travelling offenders may also make use of cloud computing to store the evidence of their encounters. In this way, they avoid the risks associated with physically transporting child sexual abuse material through airports and other checkpoints.

28. Whereas encryption measures were not previously widespread among offenders creating and distributing child sexual abuse material, for fear of being inadvertently locked out of their collections, many perpetrators are now sufficiently confident in the use of local and remote storage services that include built-in encryption technology. As a result, the trail of digital evidence that law enforcement agencies must follow may be more complex, to the extent that any digital activity, including correspondence related to offences, is encrypted or stored on remote servers instead of on local equipment. Offenders may also use new technologies to reduce permanent digital evidence. Applications such as Snapchat and Wickr enable users to send to other users temporary images that disappear within a few seconds following receipt by the receiving device. In some countries, preservation rules for maintaining SMS communications are different from rules for the retention of online electronic communications, of which offenders may also take advantage. Perpetrators are also increasingly turning to the use of Tor anonymizing networks, presenting additional challenges for tracing communications and the attribution of digital evidence to individuals.

4. Increased levels of harm for victims

29. The use of new information and communication technologies in the abuse and exploitation of children has also tended to facilitate increasing levels of harm for victims. Technologies such as peer-to-peer file-sharing have escalated the distribution of child sexual abuse material to such an extent that collections consisting of millions of images are commonplace, vastly expanding the reach of victim images. Many children feel haunted by the fact that images of their abuse are permanently accessible on the Internet.

30. An increasing level of violence and the decreasing age of the victims have also been noted. A significant number of online forums and channels openly advertise videos of brutal sexual assault. At the same time, between 2011 and 2012 there was a 70 per cent increase in child sexual abuse material focused on girls under the age of 10 years, and abuse material involving toddlers or babies is not uncommon.[6] The large amounts of readily available online child sexual abuse material may also desensitize viewers, resulting in a demand for more extreme material. Children who have been harassed, bullied or propositioned for sexual encounters are also more likely to experience unwanted exposure to harmful content, suggesting that some children suffer harm from multiple offences. In the realm of commercial sexual exploitation of children, advancements in mobile communications give perpetrators more control over their victims' movements. Offenders can require victims to call them at the beginning and end of each encounter, and the availability of global positioning systems allows offenders to monitor their victims' movements.

31. With respect to cyberenticement, the widespread use of new information and communication technologies and the immediacy of online interactions can lead perpetrators to engage in ever more direct approaches. Offenders may solicit sexual contact after a few brief interactions, unconcerned about offending or alienating some targets, and they may resort to threatening their victims into complying with their demands. For example, perpetrators may convince a child to share a compromising image and then threaten to send it to parents or to upload it to a public website in order to extort more graphic content or in-person meetings.

32. The magnitude and pervasiveness of cyberbullying have also been exacerbated in the current technological environment. Offenders use websites and social media to expand their audience and to increase the impact on the victim. Use of such platforms enables perpetrators to quickly and easily enlist others to gang up on the victim. The semi-anonymous nature of the Internet may increase the viciousness of perpetrators and aggravate the harm of the initial bullying. Children may feel that online abuse intrudes into their life without relief because unlike school, which closes at the end of the school day, technology is always "open". Victims may also hesitate to confide in their parents because they doubt their parents have a high level of technical sophistication or they fear that they will lose access to their personal technology devices. In addition, caregivers may have less opportunity to observe the abuse and intervene then they would if the abuse took place in a physical environment.

[6] "Threat assessment of child exploitation and sexual exploitation and abuse".

5. Provision of social affirmation for offenders

33. The use of new information and communication technologies provides unprecedented access to social affirmation for offenders. Whereas perpetrators in a pre-digital era would likely be ostracized from mainstream communities, there are online communities that form around all areas of abuse and exploitation, particularly with respect to child sexual abuse material and cyberenticement. Such reinforcement is particularly potent due to its immediate and interactive nature. The massive quantities of online child sexual abuse material available may also create the false impression of social acceptance, which in turn reduces the inhibitions of offenders and potential offenders. Online communities can also provide a forum for sharing strategies to gain access to victims and to evade law enforcement.

6. New forms of child abuse and exploitation

34. To a limited extent, the rise of information and communication technologies has given rise to new forms of exploitation. Some perpetrators produce "made-to-order" sexual abuse material based on age, race, sex and appearance of the victim, and offenders may specify physical settings, plot elements or sexual acts for the abuse material. Some offenders require that the child pay homage to them, for example by using the offender's name during the course of the abuse.

35. As broadband access has become widespread and relatively affordable, offenders can now stream sexual abuse of children in the form of live shows. This is demonstrated in the establishment of "cybersex" dens where children may be sexually abused by a sex tourist, and with the images being streamed on the Internet. Payment to watch these live acts is often made online with a credit card. The live format enables remote viewers to feel connected to the sexual activity. The live act can then be recorded for future distribution to maximize profit. Families can extract income by using web cameras to broadcast video or images of their children. As the offender may not consider this behaviour to constitute traditional sexual abuse, he or she may not recognize the harm that children suffer as a result.

36. The advent of the mass availability of information and communication technologies has also increased the production of, and loss of control over, self-generated content, including "sexting". "Sexting" involves the distribution of self-generated sexually explicit content, generally by mobile phone. Owing to the fact that sexting very often involves minors, it has received significant attention. As many as 15 to 40 per cent of young people report having sent such messages.[7] Recipients of such material may further distribute content without permission. Material is also obtained and distributed from children's hacked computers and other devices. In other instances, children do not know that such material is being produced and later distributed. The phenomenon is increasingly recognized as widespread, with research findings suggesting that up to 88 per cent of self-generated sexually explicit content online had been taken from its original location and uploaded elsewhere on the Internet.[8]

---

[7] Ringrose and others, *A Qualitative Study of Children, Young People and "Sexting"* (London, 2012). Available from www.nspcc.org.uk.

[8] Internet Watch Foundation, "Young people are warned they may lose control over their images and videos once they are uploaded online" (22 October 2012). Available from www.iwf.org.uk.

7. Information and communication technologies as a tool for detection

37. While the use of information and communication technologies in crimes against children poses many challenges, skilled digital investigators are able to significantly increase the detection of these types of crimes. Even when perpetrators take careful steps to avoid leaving, or to delete, digital traces, evidence may still be recoverable. In the same way as with computers, mobile device forensics can often be used to retrieve images and messages that have been deleted from a mobile phone. Depending upon data retention times, Internet Protocol (IP) connection logs can provide a complete trace of all times, sources and destinations of Internet connections.

38. In addition, abuse committed using information and communication technologies can be more likely than abuse committed offline (i.e., in person) to come to the attention of the police in the first place. Some offenders prolifically produce and publicly distribute abuse material. Parents and other caregivers might also discover abuse through digital footprints or images. Some victims themselves may even be more willing to come forward when they know that digital evidence will corroborate their claims. Online victim reporting portals that offer a non-threatening way to report abuse can be important in contributing to victim reporting.

39. When such material is encountered or reported, investigators can proactively follow leads to discover abuse, identify victims and provide victim support and assistance. Law enforcement agencies may be more willing to pursue cases if clear digital evidence of the crime confirms its severity and increases the likelihood of a successful prosecution. In that respect, it is paramount to use the information gleaned from child sexual abuse material and other digital evidence to rescue victims who remain in jeopardy.

D. Victim risk factors and offender profiles

40. Research indicates that the majority of victims of child exploitation offences are girls, although boys are increasingly at risk. Poverty and migration patterns also impact child exploitation and may be especially salient in commercial sexual exploitation of children. In terms of age, very young children and adolescents face a particularly high level of risk. Very young children are increasingly victimized in child sexual abuse material and child sex trafficking. Adolescents may face unusually high risks of cyberenticement, exposure to harmful material and cyberbullying. The extent to which children engage in risky online behaviour and neglect privacy and safety measures is a key factor affecting the degree of exploitation encountered. Prior abuse and family dysfunction also elevate the risk of victimization, particularly for commercial sexual exploitation of children. Social isolation further affects the nature of a child's online behaviour and the amount of their online activity, as well as his or her propensity to seek help when problems arise.

41. Offenders operate individually, in groups and through organized criminal networks. With respect to individual offenders, both men and women commit child exploitation offences, although men dominate in certain categories of offences, including child sexual abuse material offences, cyberenticement and cyberstalking

offences. There is a high prevalence of women offenders for certain forms of exploitation including trafficking and cyberbullying. The age range for offenders is wide, ranging from teenagers to old age. Child offending presents a particular challenge in this area, requiring both an effective justice response and a child protection-oriented response. Technical proficiency helps offenders to commit all kinds of child abuse and exploitation offences, and high levels of technical ability have been noted among offenders who illegally access personal information about children stored online.

42. The background and personal history of offenders may also play a role in offending behaviour. Although the research has sometimes yielded conflicting results, some studies show that individuals who suffered abuse as a child may be at heightened risk for offending. The age of onset and the duration of the abuse appear to affect the risk of offending, as does the degree to which the abuse was reported and addressed. Some, but not all, child exploitation offenders can be described as paedophiles (i.e., preferential child sex offenders). Others take advantage of an opportunity to offend if and when it presents itself. Poor social skills and dysfunctional relationships are common among child exploitation offenders. A vicious cycle may be at work, in which offenders with low social skills retreat into virtual social settings, thereby neglecting opportunities to improve their ability to function in the real world.

43. Groups of offenders, including organized criminal groups, most commonly focus on the production and distribution of child sexual abuse material and the commercial sexual exploitation of children. Both commercial and non-commercial groups engage in the trading of child sexual abuse material online. Commercial groups may set up web-based criminal enterprises in an attempt to profit from black market prices and a high demand for child sexual abuse material. The abuse itself may be conducted by the group or by others on a contract basis, both within their own country and in other countries, depending upon the accessibility of child victims. Organized criminal groups engaged in such offences may not depend upon traditional hierarchical organized crime models but, rather, may consist of Internet-based networks of actors who collaborate as necessary in various criminal enterprises. Nonetheless, within these loose networks, online hierarchies can form based on the criminal reputation of perpetrators for the quality of their illicit production or distribution.

44. The impact on and the protection of victims must always be at the forefront of combating technology-facilitated child abuse. Victims of physical and sexual abuse suffer a range of harm, including physical injury, psychological trauma, stigmatization, social dysfunction and a spiral of worsening situational factors. In so far as information and communication technologies facilitate existing forms of abuse, research literature on "offline" child sexual abuse can be highly relevant for at least some child exploitation offences facilitated by the new technologies. New research is needed, however, on the particular impact of such technology and especially on previously unknown forms of abuse that have emerged as a result of increased connectivity. High-priority areas in this respect include the impact of continued exposure to harmful material, as well as the nature and effect of youth-on-youth exploitation offences.

E. Combating the problem

45. Many countries face challenges in the areas of capacity and technical skills for combating these forms of crime. Nonetheless, a number of promising approaches are emerging. Efforts have been made, for example, to develop and use new technologies to share vast quantities of data between law enforcement authorities in child abuse and exploitation cases, in order to more efficiently allocate scarce human resources. Specialized software, such as PhotoDNA, generates unique codes for individual images, making it possible to effectively disrupt the online distribution of those images. Other approaches assist investigators in linking material to possible locations, victims and perpetrators, through features that appear in photographs or videos or metadata associated with electronic files.

46. Another important area is collaboration. In recent years, a number of initiatives have emerged with a view to collective problem-solving and the sharing of resources and costs. Operational collaboration in cross-border investigations is also increasing. A number of agencies, including INTERPOL and the International Centre for Missing and Exploited Children have established centralized databases to aid victim identification and investigations. Collaboration between law enforcement and private enterprises is another positive trend. Dialogue at the early stages of software product development ensures both that investigative tools most effectively meet the needs of law enforcement and that child protection considerations are taken into account in the development of online consumer products. As a result, better protection for children has been "built into" products, and private entities have been able to identify increased opportunities to support law enforcement.

47. The private sector itself engages in a number of measures to counter exploitation. Initiatives have been undertaken to establish self-regulation among Internet service providers and in the travel and tourism sectors. Civil society is also engaged in the prevention and combating of these crimes. Individuals can flag inappropriate content or call hotlines to report suspicious activity for further investigation. Parents and other caregivers have also been encouraged to contribute by talking to children about how to stay safe online, setting rules and agreeing on behaviour. Parents can also increase safety by using parental controls on social networks, online games and browsers or software that can filter or monitor what children see.

III. Assessment of the needs of States for training in the investigation of offences against children committed by using new information and communications technologies

48. As requested by the Economic and Social Council in its resolution 2011/33, the assessment of the needs of States for training in this area takes into account relevant data collected by the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime.

49. In addition, the informal expert group convened by UNODC in September 2013 to provide input to the study also discussed possible training needs in this area. The scope of possible training needs included obstacles in the identification of crimes; collection of evidence; victim assistance, protection and

cooperation; conducting efficient joint operations; international cooperation; and government structures to combat these forms of crime. The expert group indicated that, in general, there was a significant need for training related to detecting and investigating technology-facilitated child exploitation and abuse offences and for putting in place supportive government structures.

50. One of the greatest obstacles to the detection of technology-facilitated offences against children was considered to be a lack of dedicated human resources skilled in forensic investigation and able to strategically detect and investigate high-value targets. Investigations of technology-facilitated child exploitation and abuse cases are generally considered to be reactive in nature. Many members of the group noted that undercover investigations are not permitted in many countries, which creates an obstacle for law enforcement authorities because they cannot interact with possible offenders who groom children online with the intent of abuse.

51. In terms of investigative capabilities, the greatest identified obstacle was the lack of ability to obtain stored or real-time data on traffic or content, or subscriber information. The group also noted that some countries lacked expedited procedures for preserving computer data and noted the problem of the lack of formal or informal relationships with electronic service providers. Several members of the group stated that the law enforcement agencies of their country lacked sufficient resources, including access to reliable electricity, computer hardware, computer software and the Internet.

52. Specialized training for prosecutors and judges in handling digital evidence and in understanding issues common to technology-facilitated child abuse and exploitation cases was identified as a need. In particular, training was required to identify IP addresses, adapt foreign reports that use Greenwich Mean Time to local time zones, safeguard the integrity of data throughout the chain of custody, determine the relevant foreign authorities and obtain timely responses to requests for assistance, and effectively use experts to analyse digital evidence.

53. With regard to government structures, the group indicated that a specialized cybercrime unit would significantly increase the efficiency of investigation and the prosecution of these offences. One member of the expert group specified that prosecutors for such units should receive training together with investigators. Collaborative training could then serve as an opportunity to practice working together and to build informal relationships. The group also noted that an inter-agency task force on technology-facilitated child exploitation and abuse would be beneficial.

54. In terms of victim assistance, protection and cooperation, the group noted a number of opportunities to better train officials. The main deficiencies identified were the absence of standard protocols for supporting victims through the investigative process, techniques for interviewing victims, and the collection and preservation of victim-related evidence. There is a risk that untrained law enforcement agents could act with insensitivity towards victims. Further, the group noted that law enforcement agents needed training on the dynamics involved in sexual abuse and exploitation that occurs within families.

55. With respect to multijurisdictional operations, the group felt that the lack of structures such as standard operating procedures posed a major obstacle. With regard to mutual legal assistance, slow response times and channels to obtain help

for urgent mutual legal assistance requests were identified as major obstacles. The group also noted that a lack of contacts in requested countries was a problem for investigators. The group further noted a need for training on executing the formal process of mutual legal assistance requests in order to ensure the receipt of corresponding data and a need for training on the general nature and elements of international investigations.

56. The group also identified unmet needs in raising awareness among civil society. People are often confused about offensive conduct such as bullying or sexual harassment and may not know whether such conduct is actually criminalized and, if so, where to report such conduct. The group also indicated that the public and private sectors need a channel to alert police about ongoing and potential offences and that electronic service providers are not working cooperatively with law enforcement to identify and prevent even the most common offences committed on their networks.

57. The group noted that education programmes were needed to promote awareness and prevention of cybercrime. Providing training to children directly to help them to independently elude online perpetrators, as well as all forms of sexual victimization, was identified as a priority. The group also suggested increased provision of information to parents on the ways that information and communication technologies impact their children's daily life and on the crucial preventative role that they can play by paying attention to their children's concerns and interests, in order to identify warning signs of abuse or exploitation.

58. The group noted that there was an urgent need for senior officials in the criminal justice field to be made aware of the severity of the problem of technology-facilitated child exploitation and abuse and the importance of digital evidence in investigations, noting that most law enforcement agents do not realize that almost every criminal investigation involves the use of computers.

59. The group recommended that trainers carry out very specific pre-training needs assessments, especially for needs in digital forensics training. Finally, the group recommended that a single entity take a leadership role in tracking ongoing training to avoid duplication of efforts; share and build on the knowledge; collaborate with trainers in future programmes; and share materials and findings with others in the field.

IV. Conclusion

60. Our relationship with technology is constantly evolving. Thus, it is imperative that Governments, the private sector, civil society, teachers, parents and the international community consider the effects of that technology on people's lives, specifically on the lives of children. Effectively combating technology-facilitated abuse and exploitation of children will require further commitments from all stakeholders to build awareness, allocate sufficient resources to prevent and combat these crimes, establish supportive government structures, enable proactive investigations, and train practitioners on gathering, preserving and presenting electronic evidence.

V. Recommendations

61. The Commission may wish to invite Member States to do the following:

(a) Review criminal, procedural and other relevant legislation with a view to ensuring effective prevention and combat of such crimes, including enacting specific legislation or amending legislation as required;

(b) Subject to effective safeguards, enable law enforcement authorities to conduct undercover investigations to proactively address technology-facilitated grooming or solicitation of children before it becomes contact abuse;

(c) Provide training to law enforcement authorities on gathering, preserving and presenting electronic evidence in a court of law;

(d) Explore ways and means to strengthen cross-border investigations of child abuse and exploitation cases;

(e) Consider establishing specialized units within the police and prosecution offices to deal with cases of technology-facilitated child abuse and exploitation;

(f) Consider organizing an inter-agency task force on addressing the use of information and communication technologies in child abuse and exploitation;

(g) Provide training to law enforcement authorities on victim assistance and protection measures, as well as sensitive interviewing techniques;

(h) Develop, or support the development of, awareness-raising campaigns for children, parents and other caregivers.